

EVERYONE · 6 MINUTE READ

Data safety: what never to paste, and other rules

Use only approved AI tools, never paste sensitive data without permission, start with made-up examples, and keep a person in charge of important decisions.

What it is

When you type or paste something into an AI assistant, such as Claude, ChatGPT, Microsoft Copilot or Gemini, that information leaves your screen and goes to a service. Depending on the tool, your account type and your settings, it may be stored, seen by the provider or, in some consumer settings, used to improve future models. **Data safety** means knowing what you may share, where, and under which rules.

Think of a shared office building. An approved business tool is like a private meeting room with a lock. A free personal account is more like a café table: fine for general chat, not for confidential papers.

Many organisations now have an **AI policy**: rules on which tools are approved and what data they may hold. If yours does not, ask your manager before using real work data.

Why it matters

- Personal data about customers and staff is protected by law in many countries, including under data protection rules such as the GDPR in the European Union and the UK GDPR in the United Kingdom.
- Confidential information (contracts, prices, plans, passwords) can leak or be misused.
- In the European Union, the AI Act asks organisations that provide or use AI systems to take measures to support **AI literacy** among their staff. Guides like this one can be one part of that.
- Decisions with legal or customer impact need a human who can explain and stand behind them.

How to do it

1. **Use approved tools only**, through your work account, not a personal one.
2. **Check the never-paste list** below before you share anything.
3. **Start with made-up examples** when trying a new task or prompt.
4. **Anonymise** real material when you must use it: replace names, account numbers and other identifying details with labels such as [Customer A]. Replacing names lowers risk but may not make data anonymous in law; follow your policy.
5. **Check your account settings**: chat history, memory, and whether your data may be used for training. Ask IT if unsure.
6. **Read your organisation's AI policy** and ask when something is not covered.
7. **Keep a human decision** for anything affecting someone's job, money, rights, health or legal position.
8. **Report mistakes quickly**: if you pasted something you should not have, tell your manager or IT.

Example

Never paste, unless your policy explicitly allows it in that tool:

- Passwords, access codes, API keys (secret codes that let software log in)
- Bank, card or payment details
- Health information, ID numbers, home addresses
- Customer or staff personal data
- Contracts, pricing, unreleased plans and anything marked confidential
- Information shared with you under a confidentiality agreement

Before: pasting a real complaint email, with the customer's name, address and order history, into a personal AI account to draft a reply.

After, in an approved tool:

Draft a polite reply to a customer complaint. Details below are anonymised.

Customer: [Customer A]

Issue: order [number] arrived [number] days late and one item was damaged.

What we can offer: [replacement or refund, per policy]

Tone: apologetic, clear, no promises beyond the offer above.

Length: under 150 words.

You add the real details yourself in your email system, check the reply and send it under your own name.

Common mistakes

- **Using a personal account for work "just this once".** Fix: use the approved work tool, or wait.
- **Thinking deleting a chat removes the data everywhere.** Fix: assume anything shared may be kept; do not share it in the first place.
- **Anonymising badly.** Fix: remove indirect details too, such as job title plus town, that could identify someone.
- **Letting AI make decisions about people.** Fix: AI may draft or suggest; a named person decides and can explain why.
- **Assuming settings are safe by default.** Fix: check them once, and again when the tool changes.

Try it this week

1. Find your organisation's AI policy, or ask your manager whether one exists.
2. Write down which AI tools are approved for your work.
3. Open the settings of the tool you use and check history, memory and training options.
4. Take one real task and rewrite it with made-up or anonymised details.
5. Share one thing you learned with a colleague.

Going further

- Business plans often offer stronger data terms than free plans; IT can explain what your organisation has agreed.
- Connectors that link AI to email, files or systems inherit your access rights; ask for the narrowest access that does the job.
- For anything touching legal, HR or customer outcomes, involve the relevant specialist early. This guide is general information, not legal advice.

Key words

- **Approved tool:** an AI service your organisation has checked and allowed for work.
- **Personal data:** any information that can identify a living person.
- **Anonymise:** remove or replace details so a person cannot be identified, even indirectly.
- **AI policy:** your organisation's rules on using AI tools and data.
- **AI literacy:** enough understanding of AI to use it sensibly and safely in your role.